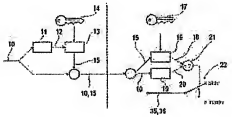
Method for activation or deactivation of microcomputer system storage arrangement, e.g. for motor vehicle control device, involves initially verifying identifier signature at start-up of computer

Publication number: DE10126451 (A1)
Publication date: 2002-12-05
Inventor(s): SCHNEIDER KLAUS [DE]; ANGERBAUER RALF [DE]; HEINDL ALEXANDER [AT] +
Applicant(s): BOSCH GMBH ROBERT [DE] +
Classification:
- International: *G06F12/14; G06F21/00; G06F21/02; G06F21/24;* G06F12/14; G06F21/00; (IPC1-7): G06F12/14
- European: G06F21/00N1C; G06F21/00N1D1
Application number: DE20011026451 20010531
Priority number(s): DE20011026451 20010531

Also published as:
US2003018905 (A1)
US6948071 (B2)
JP2003022218 (A)

Abstract of DE 10126451 (A1)

A method of activating or deactivating part (35,36) of data stored in a microcomputer system (30) involves encoding an individual microcomputer identifier (10) or filing a signature (15) in a specified memory zone (34) of the storage arrangement (32). With start-up of the computer (30), the identifier (10) signature is checked or the identifier (10) is decoded. The result of the check or decoding leads to activation or deactivation of at least part of the data An Independent claim is given for a microcomputer system with computing equipment.



(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 101 26 451 A 1**

(51) Int. Cl.[7]: G 06 F 12/14

(21) Aktenzeichen: 101 26 451.8
(22) Anmeldetag: 31. 5. 2001
(43) Offenlegungstag: 5. 12. 2002

DE 101 26 451 A 1

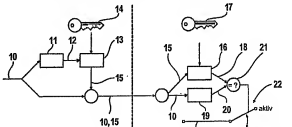
(71) Anmelder:
Robert Bosch GmbH, 70469 Stuttgart, DE

(72) Erfinder:
Schneider, Klaus, 71640 Ludwigsburg, DE; Angerbauer, Ralf, 70376 Stuttgart, DE; Heindl, Alexander, Wien, AT

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren zum Aktivieren oder Deaktivieren von in einer Speicheranordnung eines Mikrorechner-Systems abgelegten Daten

(57) Die Erfindung betrifft ein Verfahren zum Aktivieren oder Deaktivieren zumindest eines Teils (35, 36) von in einer Speicheranordnung (32) eines Mikrorechner-Systems (30) abgelegten Daten (33), insbesondere eines Teils (35, 36) eines dort abgelegten Programms. Um im Falle einer Manipulation von in der Speicheranordnung (32) abgelegten Daten (33) durch unbefugte Dritte eine Nutzung der manipulierten Daten (33) sicher und effektiv zu unterbinden, wird ein Verfahren mit den nachfolgenden Verfahrensschriften vorgeschlagen:
- eine mikrorechnerindividuelle Kennung (10, 15) wird in einem vorgebbaren Speicherbereich (34) der Speicheranordnung (32) signiert oder verschlüsselt abgelegt;
- bei einem Hochfahren des Mikrorechner-Systems (30) wird die Signatur (15) der Kennung (10) überprüft bzw. die Kennung (10) entschlüsselt; und
- in Abhängigkeit von dem Ergebnis der Überprüfung der Kennung (10) wird ein Teil der Daten (33) aktiviert bzw. deaktiviert.



DE 101 26 451 A 1

Beschreibung

Stand der Technik

[0001] Die vorliegende Erfindung betrifft ein Verfahren zum Aktivieren oder Deaktivieren zumindest eines Teils von in einer Speicheranordnung eines Mikrorechner-Systems abgelegten Daten, insbesondere eines Teils eines dort abgelegten Programms.

[0002] Die Erfindung betrifft außerdem ein Mikrorechner-System mit einem Rechengerät, insbesondere einem Mikroprozessor, und einer Speicheranordnung, in der Daten, insbesondere ein Programm, abgelegt sind.

Stand der Technik

[0003] Aus dem Stand der Technik sind Verfahren zum Schutz von in einer Speicheranordnung eines Mikrorechner-Systems abgelegten Daten, insbesondere zum Schutz eines dort abgelegten Programms, vor einer Manipulation bekannt. Derartige Verfahren werden bspw. zur Verhinderung einer unbefugten Manipulation eines in einem Steuergerät eines Kraftfahrzeugs abgelegten Steuerprogramms oder von dort abgelegten Daten eingesetzt. Das Steuerprogramm steuert oder regelt bestimmte Funktionen in dem Kraftfahrzeug, bspw. eine Brennkraftmaschine, eine Fahrdynamikregelung, ein Antiblockiersystem (ABS) oder ein elektronisches Lenksystem (Steer-by-Wire). Aufgrund einer Manipulation des Steuerprogramms kann es zu einem Defekt der gesteuerten oder geregelten Einheit des Kraftfahrzeugs kommen. Deshalb sollte eine Manipulation des Steuerprogramms oder der Daten nach Möglichkeit verhindert werden, zumindest aber sollte die Manipulation im Nachhinein erkennbar sein, damit die Ursache eines Defekts einer gesteuerten oder geregelten Einheit festgestellt werden kann bzw. damit Gewährleistungsansprüche richtig zugeordnet werden können.

[0004] Trotz der Gefahr einer Manipulation des Steuerprogramms oder der Daten durch unbefugte Personen, ist es nicht sinnvoll, den Zugriff auf die Speicheranordnung des Steuergeräts völlig zu verbieten. Um bspw. eine Neuprogrammierung des Steuergeräts vornehmen zu können, muss es einem befugten Benutzerkreis möglich sein, auf die Speicheranordnung zuzugreifen. Es kann nämlich erforderlich sein, von Zeit zu Zeit eine neue Version eines Steuerprogramms oder neue Parameter oder Grenzwerte in dem Steuergerät abzulegen, um bspw. Fehler in der Software zu beseitigen oder neuen gesetzlichen Vorgaben Rechnung zu tragen.

[0005] Bei Kraftfahrzeugsteuergeräten wird zwischen Seriengeräten und Applikationsgeräten unterschieden. Üblicherweise werden Steuergeräte nach der Fertigung als Seriengeräte ausgeliefert. Bei Seriengeräten sind Mechanismen zum Überprüfen einer Manipulation der in der Speicheranordnung des Steuergeräts abgelegten Daten aktiviert. Manipulierte Daten werden von diesen Mechanismen üblicherweise erkannt und die Daten können gesperrt werden. Die Mechanismen können ganz unterschiedlich ausgebildet sein. Aus dem Stand der Technik sind verschiedene Prüfmechanismen bekannt. In bestimmten Situationen, insbesondere während der Entwicklungs- und Erprobungsphase der Steuergeräte, ist es erforderlich, die Prüfmechanismen zu deaktivieren, damit verschiedene Daten schnell und einfach in der Speicheranordnung abgelegt werden können. Ein Steuergerät mit deaktivierten Prüfmechanismen wird als ein Applikationsgerät bezeichnet.

[0006] Um eine lücklose Testabdeckung der in der Speicheranordnung abgelegten Daten sicherstellen zu können,

müssen im Serienfall und im Applikationsfall die gleichen Daten, insbesondere muss das gleiche Steuerprogramm, in der Speicheranordnung des Steuergeräts abgelegt sein. Deshalb muss es möglich sein, ein Steuergerät von einem Serienfall in einen Applikationsfall umschalten zu können, ohne andere Daten in die Speicheranordnung laden zu müssen. Ein Umschalten vom Applikationsfall zurück in den Serienfall ist nicht erwünscht und sollte nach Möglichkeit sogar unmöglich sein, um zu verhindern, dass Steuergeräte in Umlauf sind, deren Steuerprogramm von dem Hersteller der Steuergeräte nicht getestet und genehmigt wurde.

[0007] Nach dem Stand der Technik sind Applikationsgeräte durch einen Eintrag in einem geheimen nicht-flüchtigen Speicherbereich der Speicheranordnung des Steuergeräts gekennzeichnet. Der geheime Speicherbereich befindet sich außerhalb des im Rahmen einer Neuprogrammierung des Steuergeräts zu programmierenden Speicherbereichs der Speicheranordnung. Je nach dem, ob es sich um ein Seriengerät oder ein Applikationsgerät handelt, wird der geheime Speicherbereich im Anschluß an eine Erstprogrammierung der Speicheranordnung bzw. durch ein entsprechendes Verfahren angestoßen beim Hochfahren des Steuergeräts mit einem entsprechenden Eintrag programmiert.

[0008] Bei einem nachfolgenden Hochfahren des Steuergeräts wird dann nur noch der Eintrag in dem geheimen Speicherbereich überprüft und in Abhängigkeit von dem Eintrag zwischen einem Serienfall und einem Applikationsfall umgeschaltet, d. h. die Prüfmechanismen werden aktiviert bzw. deaktiviert. Wenn in dem geheimen Speicherbereich kein Eintrag vorhanden ist, wird von einem Serienfall ausgegangenen und die Prüfmechanismen werden aktiviert. Bei den bekannten Steuergeräten kann also durch Beschreiben des geheimen Speicherbereichs mit einem entsprechenden Eintrag von einem Serienfall in einen Applikationsfall umgeschaltet werden.

[0009] Der Umschaltvorgang von einem Serienfall in einen Applikationsfall durch Beschreiben des geheimen Speicherbereichs kann bei den bekannten Steuergeräten jedoch relativ problemlos aufgezeichnet werden. Von besonderem Interesse ist dabei der Eintrag, der in dem geheimen Speicherbereich eines Applikationsgeräts abgelegt ist. Bei den aus dem Stand der Technik bekannten Verfahren zum Aktivieren oder Deaktivieren von in einer Speicheranordnung eines Mikrorechner-Systems abgelegten Daten kann der Eintrag aus einem Applikationsgerät ausgelesen und dazu genutzt werden, weitere Steuergeräte in den Applikationsfall mit deaktivierten Prüfmechanismen umzuschalten. Auf diesen manipulierten Applikationsgeräten können manipulierte Daten abgelegt und die manipulierten Daten dann ausgeführt bzw. genutzt werden. Die manipulierten Daten können nicht zuverlässig vor einer Nutzung geschützt werden.

[0010] Deshalb ist es eine Aufgabe der vorliegenden Erfindung, im Falle einer Manipulation von in der Speicheranordnung abgelegten Daten durch unbefugte Dritte, eine Nutzung der manipulierten Daten sicher und effektiv zu unterbinden.

[0011] Zur Lösung dieser Aufgabe schlägt die Erfindung ausgehend von dem Verfahren der eingangs genannten Art die nachfolgenden Verfahrensschritte vor:

- eine mikrorechnerindividuelle Kennung wird verschlüsselt oder eine Signatur einer mikrorechnerindividuellen Kennung wird in einem vorgebbaren Speicherbereich der Speicheranordnung abgelegt;
- bei einem Hochfahren des Mikrorechner-Systems wird die Signatur der Kennung überprüft bzw. die Kennung entschlüsselt; und
- in Abhängigkeit von dem Ergebnis der Überprüfung

der Signatur bzw. von der entschlüsselten Kennung wird zumindest ein Teil der Daten aktiviert oder deaktiviert.

Vorteile der Erfindung

[0012] Gemäß der vorliegenden Erfindung wird also ein Eintrag in einen Speicherbereich der Speicheranordnung signiert bzw. verschlüsselt vorgenommen. Der Eintrag kann in einen beliebigen Speicherbereich der Speicheranordnung abgelegt werden. Das Ablegen des verschlüsselten Eintrags kann im Anschluß an eine Neu- oder Umprogrammierung erfolgen oder durch ein entsprechendes Verfahren angestoßen werden. Die Sicherheit des erfindungsgemäßen Verfahrens ist vor allem durch die Signierung oder Verschlüsselung des Eintrags mit einem geheimen Schlüssel und nicht durch die Geheimhaltung der Adresse des Speicherbereichs gegeben. Der Speicherbereich sollte bei einer Neuprogrammierung der Speicheranordnung zwar gelöscht, aber nicht mit den neuen Daten beschrieben werden. Das Mikrorechner-System ist bspw. als eine Steuergerät zum Steuern und/oder Regeln von Kraftfahrzeugfunktionen ausgebildet.

[0013] Beim Hochfahren des Mikrorechner-Systems wird die Signatur des Eintrags überprüft bzw. der Eintrag entschlüsselt. Wenn kein Eintrag in dem Speicherbereich vorhanden ist oder die Überprüfung der Signatur des dort abgelegten Eintrags oder die Entschlüsselung des Eintrags fehlgeschlagen ist, wird von einem Serienfall ausgegangen und die Prüfmechanismen werden aktiviert. Wenn dagegen die Überprüfung der Signatur des in dem Speicherbereich abgelegten Eintrags oder die Entschlüsselung des Eintrags erfolgreich war, wird von einem Applikationsfall ausgegangen und die Prüfmechanismen werden deaktiviert. Erfindungsgemäß kann also durch Ablegen eines entsprechenden verschlüsselten Eintrags in einen vorgehbaren Speicherbereich der Speicheranordnung von einem Steuergerät auf ein Applikationsgerät umgeschaltet werden.

[0014] Mit dem erfindungsgemäßen Verfahren kann ein Steuergerät nicht nur zwischen Serienfall und Applikationsfall umgeschaltet werden. Es ist auch denkbar, über den verschlüsselten Eintrag in den Speicherbereich beliebige Teile der Daten und damit beliebige Funktionen eines Programms zu aktivieren bzw. zu deaktivieren. Dadurch ist es bspw. Kraftfahrzeugherstellern möglich, durch einen gezielten Eingriff in das Steuerprogramm eines Kraftfahrzeugsteuergeräts verschiedene Kraftfahrzeugfunktionen, z. B. verschiedene Leistungen der Brennkraftmaschine, zu realisieren. Mit der vorliegenden Erfindung können also beliebige Funktionen eines Programms über Softwareschalter, die nur von befugten Personen betätigt werden können, aktiviert bzw. deaktiviert werden.

[0015] Gemäß einer vorteilhaften Weiterbildung der vorliegenden Erfindung wird vorgeschlagen, dass zum Aktivieren oder Deaktivieren unterschiedlicher Teile von Daten verschiedene Kennungen in dem Speicherbereich der Speicheranordnung abgelegt werden. Die verschiedenen Funktionen eines Programms werden also über den Inhalt des Speicherbereichs aktiviert bzw. deaktiviert.

[0016] Gemäß einer anderen vorteilhaften Weiterbildung der vorliegenden Erfindung wird vorgeschlagen, dass zum Aktivieren oder Deaktivieren unterschiedlicher Teile von Daten eine Kennung in verschiedene Speicherbereiche der Speicheranordnung abgelegt wird. Die verschiedenen Funktionen eines Programms werden also über den Speicherbereich aktiviert bzw. deaktiviert, in dem die Kennung abgelegt ist. Es ist auch denkbar, verschiedene Kennungen in verschiedenen Speicherbereichen abzulegen, um auf diese Weise mit möglichst wenig Speicherplatz möglichst viele Programmfunktionen aktivieren bzw. deaktivieren zu können.

[0017] Gemäß einer bevorzugten Ausführungsform der vorliegenden Erfindung wird vorgeschlagen, dass anhand eines lediglich einem beschränkten Personenkreis zugänglichen privaten Schlüssels die mikrorechnerindividuelle Kennung signiert oder verschlüsselt wird und anhand eines frei zugänglichen öffentlichen Schlüssel die Signatur der Kennung überprüft bzw. die Kennung entschlüsselt wird. Gemäß dieser Ausführungsform wird die Kennung nach einem asymmetrischen Verschlüsselungsverfahren signiert bzw. verschlüsselt. Das asymmetrische Verschlüsselungsverfahren wird auch als Public-Key-Verschlüsselungsverfahren bezeichnet. Asymmetrische Verschlüsselungsverfahren sind bspw. RSA (benannt nach den Entwicklern dieses Verfahrens Ronald Rivest, Adi Shamir und Leonard Adleman; Verschlüsseln durch modulares Potenzieren $c = m^e \bmod n$), LUC (ähnlich RSA; Verschlüsseln durch Bildung der Lucas-Folge) oder MNLN (Müller, Nöbauer, Lidl, Nöbauer; wie RSA, aber Polynom x^e wird durch Dickson-Polynom ersetzt) (vgl. http://www.uni-mainz.de/~pommeren/DSVorlesung/KryptoBasis/asymmetrisch.html).

[0018] Bei dem asymmetrischen Verschlüsselungsverfahren wird bspw. zum Signieren eines Steuerprogramms für ein Steuergerät eines Kraftfahrzeugs aus dem zu signierenden Steuerprogramm und/oder den zu signierenden Daten mit Hilfe einer Hash-Funktion ein Hash-Wert gebildet. Ein Hash-Wert ist eine Art Prüfsumme mit besonderen Eigenschaften, die von der verwendeten Hash-Funktion abhängig sind. Der Hash-Wert wird mit Hilfe eines nicht frei zugänglichen privaten Schlüssels verschlüsselt. Der verschlüsselte Hash-Wert wird als Signatur bezeichnet. Die Signatur wird an das zu signierende Programm und/oder die zu signierenden Daten angehängt und zusammen mit diesen an das Kraftfahrzeugsteuergerät übertragen und dort in der Speicheranordnung gespeichert.

[0019] In dem Steuergerät wird die Signatur mit Hilfe eines frei zugänglichen öffentlichen Schlüssels wieder entschlüsselt. Dadurch erhält man den entschlüsselten Hash-Wert. Außerdem wird mit Hilfe derselben Hash-Funktion, die auch im Rahmen der Verschlüsselung zum Ermitteln des Hash-Wertes eingesetzt wurde, aus dem empfangenen Steuerprogramm und/oder den empfangenen Daten ein weiterer Hash-Wert ermittelt. Anschließend wird überprüft, ob der entschlüsselte Hash-Wert gleich dem weiteren Hash-Wert ist. Falls dem so ist, wird die Ausführung des übertragenen Steuerprogramms bzw. die Nutzung der übertragenen Daten freigegeben. Anderenfalls wird die Ausführung des Steuerprogramms bzw. die Nutzung der Daten gesperrt.

[0020] Vorteilhafterweise wird die Kennung in einem Speicherbereich der Speicheranordnung abgelegt, der während der Nutzung der Daten nicht verändert wird. Auf dem Speicherbereich wird also während der Ausführung des Programms weder lesend noch schreibend zugegriffen.

[0021] Vorzugsweise wird die Kennung in einem Speicherbereich abgelegt, der im Rahmen einer Neuprogrammierung der Speicheranordnung gelöscht wird. Im Anschluss an eine Neuprogrammierung muss also die mikrorechnerindividuelle Kennung in dem vorgebbaren Speicherbereich der Speicheranordnung signiert oder verschlüsselt abgelegt werden. Dazu muss einerseits die individuelle Kennung des Mikrorechner-Systems und andererseits auch der richtige Verschlüsselungsalgorithmus und der richtige Schlüssel bekannt sein. Eine Ausführung oder Nutzung der neu programmierten Daten ist also nur dann nicht gesperrt, wenn die richtige Kennung mit dem richtigen Schlüssel und Algorithmus signiert oder verschlüsselt in dem Speicherbe-

reich der Speicheranordnung abgelegt worden ist.

[0022] Gemäß einer bevorzugten Ausführungsform der vorliegenden Erfindung wird vorgeschlagen, dass bei jedem Hochfahren des Mikrorechner-Systems die Signatur der Kennung überprüft bzw. die Kennung entschlüsselt wird.

[0023] Vorteilhafterweise wird eine dem Mikrorechner-System zugeordnete Seriennummer, insbesondere eine dem Rechengerät des Mikrorechner-Systems zugeordnete Seriennummer, in dem vorgebbaren Speicherbereich der Speicheranordnung signiert oder verschlüsselt abgelegt.

[0024] Gemäß einer bevorzugten Ausführungform der vorliegenden Erfindung wird vorgeschlagen, dass in dem Mikrorechner-System Mechanismen zum Überprüfen einer Manipulation der in der Speicheranordnung abgelegten Daten aktiviert werden, falls in dem Speicherbereich der Speicheranordnung keine Kennung abgelegt ist oder falls die Überprüfung der Signatur der dort abgelegten Kennung oder die Entschlüsselung der dort abgelegten Kennung beim Hochfahren des Mikrorechner-Systems scheitert. In diesen Fällen wird also ein als Kraftfahrzeugsteuergerät ausgebildetes Mikrorechner-System in den Serienfall geschaltet. Falls die vorgesehenen Prüfmechanismen eine Manipulation der Daten erkennen, wird die Ausführung oder Nutzung der neu programmierten Daten blockiert.

[0025] Gemäß einer weiteren bevorzugten Ausführungsform der vorliegenden Erfindung wird vorgeschlagen, dass in dem Mikrorechner-System Mechanismen zum Überprüfen einer Manipulation der in der Speicheranordnung abgelegten Daten deaktiviert werden, falls die Überprüfung der Signatur der in dem Speicherbereich der Speicheranordnung abgelegten Kennung oder die Entschlüsselung der dort abgelegten Kennung beim Hochfahren des Mikrorechner-Systems erfolgreich ist. In diesem Fall wird also ein als Kraftfahrzeugsteuergerät ausgebildetes Mikrorechner-System in den Applikationsfall geschaltet.

[0026] Als eine weitere Lösung der Aufgabe der vorliegenden Erfindung wird ausgehend von dem Mikrorechner-System der eingangs genannten Art vorgeschlagen, dass

- in einem vorgebbaren Speicherbereich der Speicheranordnung eine mikrorechnerindividuelle Kennung signiert oder verschlüsselt abgelegt ist;
- Mittel zum Überprüfen der Signatur der Kennung bzw. zum Entschlüsseln der Kennung bei einem Hochfahren des Mikrorechner-Systems; und
- Mittel zum Aktivieren oder Deaktivieren zumindest eines Teils der in der Speicheranordnung des Mikrorechner-Systems abgelegten Daten in Abhängigkeit von dem Ergebnis der Überprüfung der Signatur bzw. von der entschlüsselten Kennung

vorgesehen sind.

[0027] Gemäß einer vorteilhaften Weiterbildung der vorliegenden Erfindung wird vorgeschlagen, dass das Mikrorechner-System als ein Steuergerät für ein Kraftfahrzeug zur Steuerung und/oder Regelung von Kraftfahrzeugfunktionen ausgebildet ist.

[0028] Gemäß einer bevorzugten Ausführungsform der vorliegenden Erfindung wird vorgeschlagen, dass das Mikrorechner-System Mittel zur Ausführung des erfindungsgemäßen Verfahrens aufweist.

[0029] Vorteilhafterweise ist in der Speicheranordnung ein Computerprogramm abgelegt, das auf dem Rechengerät ablauffähig und zur Ausführung des erfindungsgemäßen Verfahrens geeignet ist.

[0030] Vorzugsweise ist die Speicheranordnung auf dem gleichen Halbleiterbauelement ausgebildet wie das Rechengerät. Bei einem solchen sog. On-Chip-Speicher kann der Programmspeicher bzw. können die darauf abgelegten Daten nicht von außen manipuliert werden, wodurch das Mikrorechner-System zusätzlich gegen Manipulation der auf der Speicheranordnung abgelegten Daten geschützt ist.

Zeichnungen

[0031] Weitere Merkmale, Anwendungsmöglichkeiten und Vorteile der Erfindung ergeben sich aus der nachfolgenden Beschreibung von Ausführungsbeispielen der Erfindung, die in der Zeichnung dargestellt sind. Dabei bilden alle beschriebenen oder dargestellten Merkmale für sich oder in beliebiger Kombination den Gegenstand der Erfindung, unabhängig von ihrer Zusammenfassung in den Patentansprüchen oder deren Rückbeziehung sowie unabhängig von ihrer Formulierung bzw. Darstellung in der Beschreibung bzw. in der Zeichnung. Es zeigen:

[0032] Fig. 1 ein Ablaufdiagramm eines erfindungsgemäßen Verfahrens gemäß einer bevorzugten Ausführungsform;

[0033] Fig. 2 ein weiteres Ablaufdiagramm des Verfahrens aus Fig. 1; und

[0034] Fig. 3 ein erfindungsgemäßes Mikrorechner-System gemäß einer bevorzugten Ausführungsform.

Beschreibung der Ausführungsbeispiele

[0035] Gegenstand der vorliegenden Erfindung ist ein Verfahren zum Aktivieren oder Deaktivieren zumindest eines Teils von Daten, die in einer Speicheranordnung eines Mikrorechner-Systems abgelegt sind. Das Mikrorechner-System ist bspw. als ein Steuergerät eines Kraftfahrzeugs zur Steuerung und/oder Regelung bestimmter Kraftfahrzeugfunktionen ausgebildet. Die Daten sind bspw. als ein Steuerprogramm, als Grenzwerte oder als Parameterwerte ausgebildet.

[0036] Durch aktivieren bzw. deaktivieren von Teilen des Steuerprogramms können verschiedene Funktionen des Steuergeräts ein- bzw. ausgeschaltet werden. Insbesondere ist daran gedacht, durch Aktivieren bzw. Deaktivieren von Teilen des Steuerprogramms das Steuergerät von einem Serienfall in einen Applikationsfall zu schalten. Bei Seriengeräten sind Mechanismen zum Überprüfen einer Manipulation der in einer Speicheranordnung des Steuergeräts abgelegten Daten aktiviert. Manipulierte Daten werden von diesen Mechanismen erkannt und die Daten können gesperrt werden. Die Mechanismen können ganz unterschiedlich ausgebildet sein. Aus dem Stand der Technik sind viele unterschiedliche Prüfmechanismen bekannt. In bestimmten Situationen, insbesondere während der Entwicklungs- und Erprobungsphase der Steuergeräte, ist es erforderlich, die Prüfmechanismen zu deaktivieren, damit verschiedene Daten schnell und einfach in der Speicheranordnung abgelegt werden können. Ein Steuergerät mit deaktivierten Prüfmechanismen wird als Applikationsgerät bezeichnet.

[0037] Das in Fig. 1 dargestellte erfindungsgemäße Verfahren beginnt in einem Funktionsblock 1. In einem Funktionsblock 2 wird eine mikrorechnerindividuelle Kennung mit Hilfe eines privaten Schlüssels nach einem asymmetrischen Verschlüsselungsverfahren signiert oder verschlüsselt. Die signierte oder verschlüsselte Kennung wird als Zertifikat bezeichnet. Die Kennung ist bspw. eine Seriennummer des Steuergeräts oder eines Rechengeräts, insbesondere eines Mikroprozessors, des Steuergeräts. Die Verschlüsselung der Kennung wird an Hand der Fig. 2 im Detail beschrieben. In einem Funktionsblock 3 wird bei einem Hochfahren des Steuergeräts mit Hilfe eines öffentlichen Schlüssels die Signatur der Kennung geprüft bzw. die Kennung entschlüsselt. In einem Abfrageblock 4 wird dann überprüft,

ob die Signatur der Kennung in Ordnung ist oder ob die entschlüsselte Kennung mit der tatsächlichen Kennung des Mikrorechner-Systems übereinstimmt. Falls das der Fall ist, ist das Steuergerät ein Applikationsgerät, und in einem Funktionsblock **5** werden sämtliche Prüfmechanismen deaktiviert. Falls jedoch in dem Speicherbereich keine Kennung vorhanden ist, die Signatur fehlerhaft oder die entschlüsselte Kennung nicht mit der tatsächlichen Kennung übereinstimmt, ist das Steuergerät ein Seriengerät, und in einem Funktionsblock **6** werden die Prüfmechanismen aktiviert. Bei einer zukünftigen Ausführung oder Nutzung der in der Speicheranordnung abgelegten Daten werden die Daten auf eine Manipulation hin untersucht. In der Regel werden manipulierte Daten erkannt und blockiert, so dass eine Ausführung oder Nutzung nicht mehr möglich ist. In den Funktionsblöcken **3** bis **6** wird also in Abhängigkeit von der Kennung ein Teil des Steuerprogramms aktiviert bzw. deaktiviert. In einem Funktionsblock **7** ist das erfindungsgemäße Verfahren dann beendet.

[0038] In Fig. **2** ist ein weiteres Ablaufdiagramm des Verfahrens aus Fig. **1** dargestellt, wobei insbesondere die Signierung bzw. die Verschlüsselung der Daten und die Überprüfung der Signatur bzw. die Entschlüsselung der Daten im Detail dargestellt ist. Aus einer Seriennummer **10** des Mikroprozessors des Steuergeräts wird in einem Funktionsblock **11** mit Hilfe einer Hash-Funktion ein sog. Hash-Wert **12** gebildet. Der Hash-Wert **12** wird in einem Funktionsblock **13** mit Hilfe des privaten Schlüssels **14** verschlüsselt. Der verschlüsselte Hash-Wert wird als Signatur **15** bezeichnet. Die Signatur **15** wird an die Seriennummer **10** angehängt, beide werden über eine geeignete Datenschnittstelle an das Steuergerät eines Kraftfahrzeugs übertragen und dort in einem vorgegebenen Speicherbereich der Speicheranordnung abgelegt.

[0039] In dem Steuergerät wird die Seriennummer **10** von der Signatur **15** getrennt. Die Signatur **15** wird in einem Funktionsblock **16** mit Hilfe eines öffentlichen Schlüssels **17** entschlüsselt. Der entschlüsselte Hash-Wert ist mit dem Bezugszeichen **18** bezeichnet. In einem Funktionsblock **19** wird aus der Seriennummer **10** anhand derselben Hash-Funktion, wie sie auch in dem Funktionsblock **11** eingesetzt wurde, ein weiterer Hash-Wert **20** ermittelt. In einem Abfrageblock **21** wird überprüft, ob der entschlüsselte Hash-Wert **18** gleich dem ermittelten Hash-Wert **20** ist, d. h. ob die entschlüsselte Seriennummer gleich der tatsächlichen Seriennummer **10** des Mikroprozessors des Steuergeräts ist. Falls das der Fall ist, wird das Steuergerät in den Applikationsfalls geschaltet. Dazu werden Prüfmechanismen **35**, **36** zum Überprüfen der in der Speicheranordnung abgelegten Daten auf Manipulation mit Hilfe eines von dem Abfrageblock **21** angesteuerten Schaltelements **22** deaktiviert. Anderenfalls wird das Steuergerät in den Serienfall geschaltet, indem die Prüfmechanismen **35**, **36** mit Hilfe des Schaltelements **22** aktiviert.

[0040] Der private Schlüssel **14** steht nur einem beschränkten Personenkreis zur Verfügung. Zur Erhöhung der Sicherheit ist es denkbar, die privaten Schlüssel **14** in einem Trust-Centre zu verwalten und die Seriennummer **10** mit Hilfe eines Signatur-Servers des Trust-Centres zu signieren. Ein entsprechendes Verfahren ist in einer separaten Patentanmeldung DE 101 23 169 der gleichen Anmelderin mit Anmeldetag 12. Mai 2001 beschrieben. Auf den Inhalt dieser Anmeldung wird ausdrücklich Bezug genommen.

[0041] Alternativ kann die Kennung **10** mit Hilfe des privaten Schlüssels **14** auch direkt verschlüsselt werden. Die verschlüsselte Kennung wird an das Steuergerät übertragen und dort mit Hilfe des öffentlichen Schlüssel **17** direkt entschlüsselt. In Abhängigkeit von der entschlüsselten Kennung **10** wird in dem Steuergerät über das Schaltelement **22** dann zumindest ein Teil der in der Speicheranordnung abgelegten Daten aktiviert oder deaktiviert.

[0042] In Fig. **3** ist ein erfindungsgemäßes Mikrorechner-System in seiner Gesamtheit mit dem Bezugszeichen **30** bezeichnet. Das Mikrorechner-System **30** ist als ein Steuergerät für ein Kraftfahrzeug zur Steuerung und/oder Regelung von Kraftfahrzeugfunktionen ausgebildet. Das Steuergerät **30** umfasst ein Rechengerät **31**, das insbesondere als ein Mikroprozessor ausgebildet ist, und eine Speicheranordnung **32**, in der verschiedene Daten **33**, insbesondere ein Steuerprogramm, Grenzwerte oder Parameterwerte, abgelegt sind. Die Speicheranordnung **32** ist auf dem gleichen Halbleiterbauelement ausgebildet wie der Mikroprozessor **31** (On-Chip-Speicher). In einem vorgebbaren Speicherbereich **34** der Speicheranordnung **32** ist eine mikrorechnerindividuelle Kennung **10**, insbesondere eine Seriennummer des Mikroprozessors **31** (CPU-Seriennummer), signiert oder verschlüsselt abgelegt. Der Speicherbereich **34** wird im Rahmen einer Neuprogrammierung der Speicheranordnung **32** automatisch gelöscht, jedoch nicht mit neuen Daten beschrieben. Während der Nutzung der Daten **33**, d. h. während der Ausführung des Steuerprogramms, wird der Inhalt des Speicherbereichs **34** nicht verändert.

[0043] Beim Hochfahren des Steuergeräts **30** wird die Signatur **15** der Kennung **10** überprüft bzw. die Kennung **10** entschlüsselt. Dazu sind in dem Steuergerät **30** geeignete Mittel vorgesehen, die bei jedem Hochfahren des Steuergeräts **30** den Inhalt des Speicherbereichs **34** überprüfen. In Abhängigkeit von dem Inhalt des Speicherbereichs **34** werden durch entsprechende Mittel des Steuergeräts **30** bestimmte Teile **35**, **36** des Steuerprogramms **33** aktiviert bzw. deaktiviert. Die Teile **35**, **36** sind bspw. Prüfmechanismen, durch die die übrigen in der Speicheranordnung **34** abgelegten Daten **33** auf eine Manipulation hin geprüft werden können.

[0044] Falls in dem Speicherbereich **34** keine Kennung **10**, **15** abgelegt ist oder falls die Überprüfung der Signatur **15** oder das Entschlüsseln der Kennung **10** ergibt, dass die Kennung **10**, **15** mit einem falschen privaten Schlüssel **14** signiert oder verschlüsselt worden ist, wird das Steuergerät **30** in einen Serienfall geschaltet, indem die Teile **35**, **36** des Steuerprogramms **33** aktiviert werden. Anderenfalls wird das Steuergerät **30** in einen Applikationsfall geschaltet, indem die Teile **35**, **36** des Steuerprogramms **33** deaktiviert werden.

[0045] Bei der Auslieferung des Steuergeräts **30** ist der Speicherbereich **34** der Speicheranordnung **32** leer. Es handelt sich also um ein Seriengerät mit aktiven Prüfmechanismen. Falls das Seriengerät in ein Applikationsgerät mit inaktiven Prüfmechanismen umgeschaltet werden soll, wird die Seriennummer des Mikroprozessors **31** des Steuergeräts **30** signiert oder verschlüsselt in dem Speicherbereich **34** abgelegt. Dazu ist der richtige private Schlüssel **14** erforderlich, der nur einem beschränkten Personenkreis zugänglich ist.

[0046] Vorzugsweise ist in der Speicheranordnung **32** ein Computerprogramm abgelegt, das auf dem Rechengerät **31** ablauffähig und zur Ausführung der nachfolgenden Verfahrensschritte geeignet ist:

- Ablegen der signierten oder verschlüsselten mikrorechnerindividuellen Kennung **10**, **15** in dem vorgebbaren Speicherbereich **34** der Speicheranordnung **32**;
- Überprüfen der Signatur **15** der Kennung **10** bzw. Entschlüsseln der Kennung **10** beim Hochfahren des Mikrorechner-Systems **30**; und
- Aktivieren bzw. Deaktivieren zumindest eines Teils

der in der Speicheranordnung **32** abgelegten Daten in Abhängigkeit von dem Inhalt des Speicherbereichs **34**.

[0047] Die in der Speicheranordnung **32** abgelegten Daten werden also in Abhängigkeit von dem Ergebnis der Überprüfung der Signatur **15** bzw. in Abhängigkeit von der entschlüsselten Kennung **10** aktiviert bzw. deaktiviert.

Patentansprüche

1. Verfahren zum Aktivieren oder Deaktivieren zumindest eines Teils (**35**, **36**) von in einer Speicheranordnung (**32**) eines Mikrorechner-Systems (**30**) abgelegten Daten (**33**), insbesondere eines Teils (**35**, **36**) eines dort abgelegten Programms, **gekennzeichnet durch** die nachfolgenden Verfahrensschritte:
   - eine mikrorechnerindividuelle Kennung (**10**) wird verschlüsselt oder eine Signatur (**15**) einer mikrorechnerindividuellen Kennung (**10**) wird in einem vorgebbaren Speicherbereich (**34**) der Speicheranordnung (**32**) abgelegt;
   - bei einem Hochfahren des Mikrorechner-Systems (**30**) wird die Signatur (**15**) der Kennung (**10**) überprüft bzw. die Kennung (**10**) entschlüsselt; und
   - in Abhängigkeit von dem Ergebnis der Überprüfung der Signatur (**15**) bzw. von der entschlüsselten Kennung (**10**) wird zumindest ein Teil der Daten (**33**) aktiviert oder deaktiviert.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass zum Aktivieren oder Deaktivieren unterschiedlicher Teile (**35**, **36**) von Daten (**33**) verschiedene Kennungen in dem Speicherbereich (**34**) der Speicheranordnung (**32**) abgelegt werden.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass zum Aktivieren oder Deaktivieren unterschiedlicher Teile (**35**, **36**) von Daten (**33**) eine Kennung (**10**) in verschiedene Speicherbereiche (**34**) der Speicheranordnung (**32**) abgelegt wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass anhand eines lediglich einem beschränkten Personenkreis zugänglichen privaten Schlüssels (**14**) die mikrorechnerindividuelle Kennung (**10**, **15**) signiert oder verschlüsselt wird und anhand eines frei zugänglichen öffentlichen Schlüssel (**17**) die Signatur (**15**) der Kennung (**10**) überprüft bzw. die Kennung (**10**) entschlüsselt wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass die Kennung (**10**, **15**) in einem Speicherbereich (**34**) der Speicheranordnung (**32**) abgelegt wird, der während der Nutzung der Daten (**33**) nicht verändert wird.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Kennung (**10**, **15**) in einem Speicherbereich (**34**) abgelegt wird, der im Rahmen einer Neuprogrammierung der Speicheranordnung (**32**) gelöscht wird.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass bei jedem Hochfahren des Mikrorechner-Systems (**30**) die Signatur (**15**) der Kennung (**10**) überprüft bzw. die Kennung (**10**) entschlüsselt wird.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass eine dem Mikrorechner-System (**30**) zugeordnete Seriennummer, insbesondere eine dem Rechengerät (**31**) des Mikrorechner-Systems (**30**) zugeordnete Seriennummer, in dem vorgebbaren Speicherbereich (**34**) der Speicheranordnung (**32**) signiert oder verschlüsselt abgelegt wird.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass in dem Mikrorechner-System (**30**) Mechanismen zum Überprüfen einer Manipulation der in der Speicheranordnung (**32**) abgelegten Daten (**33**) aktiviert werden, falls in dem Speicherbereich (**34**) der Speicheranordnung (**32**) keine Kennung (**10**, **15**) abgelegt ist oder falls die Überprüfung der Signatur (**15**) der dort abgelegten Kennung (**10**) oder die Entschlüsselung der dort abgelegten Kennung (**10**) beim Hochfahren des Mikrorechner-Systems (**30**) scheitert.

10. Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass in dem Mikrorechner-System (**30**) Mechanismen zum Überprüfen einer Manipulation der in der Speicheranordnung (**32**) abgelegten Daten (**33**) deaktiviert werden, falls die Überprüfung der Signatur (**15**) der in dem Speicherbereich (**34**) der Speicheranordnung (**32**) abgelegten Kennung (**10**) oder die Entschlüsselung der dort abgelegten Kennung (**10**) beim Hochfahren des Mikrorechner-Systems (**30**) erfolgreich ist.

11. Mikrorechner-System (**30**) mit einem Rechengerät (**31**), insbesondere einem Mikroprozessor, und einer Speicheranordnung (**32**), in der Daten (**33**), insbesondere ein Programm, abgelegt sind, gekennzeichnet durch
   eine in einem vorgebbaren Speicherbereich (**34**) der Speicheranordnung (**32**) signiert oder verschlüsselt abgelegte mikrorechnerindividuelle Kennung (**10**, **15**);
   Mittel zum Überprüfen der Signatur (**15**) der Kennung (**10**) bzw. zum Entschlüsseln der Kennung (**10**) bei einem Hochfahren des Mikrorechner-Systems (**30**); und
   Mittel zum Aktiveren oder Deaktiveren zumindest eines Teils (**35**, **36**) der in der Speicheranordnung (**32**) des Mikrorechner-Systems (**30**) abgelegten Daten (**33**) in Abhängigkeit von dem Ergebnis der Überprüfung der Signatur (**15**) bzw. von der entschlüsselten Kennung (**10**).

12. Mikrorechner-System (**30**) nach Anspruch 11, dadurch gekennzeichnet, dass das Mikrorechner-System (**30**) als ein Steuergerät für ein Kraftfahrzeug zur Steuerung und/oder Regelung von Kraftfahrzeugfunktionen ausgebildet ist.

13. Mikrorechner-System (**30**) nach Anspruch 11 oder 12, dadurch gekennzeichnet, dass das Mikrorechner-System (**30**) Mittel zur Ausführung eines Verfahrens nach einem der Ansprüche 2 bis 10 aufweist.

14. Mikrorechner-System (**30**) nach einem der Ansprüche 11 bis 13, dadurch gekennzeichnet, dass in der Speicheranordnung (**32**) ein Computerprogramm abgelegt ist, das auf dem Rechengerät (**31**) ablauffähig und zur Ausführung eines Verfahrens nach einem der Ansprüche 1 bis 10 geeignet ist.

15. Mikrorechner-System (**30**) nach einem der Ansprüche 11 bis 14, dadurch gekennzeichnet, dass die Speicheranordnung (**32**) auf dem gleichen Halbleiterbauelement ausgebildet ist wie das Rechengerät (**31**).

Hierzu 3 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 101 26 451 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 5. Dezember 2002

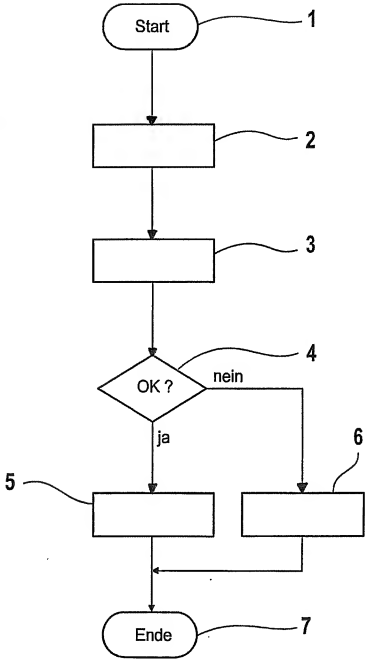


FIG. 1

Nummer: DE 101 26 451 A1
Int. Cl.7: G 06 F 12/14
Offenlegungstag: 5. Dezember 2002

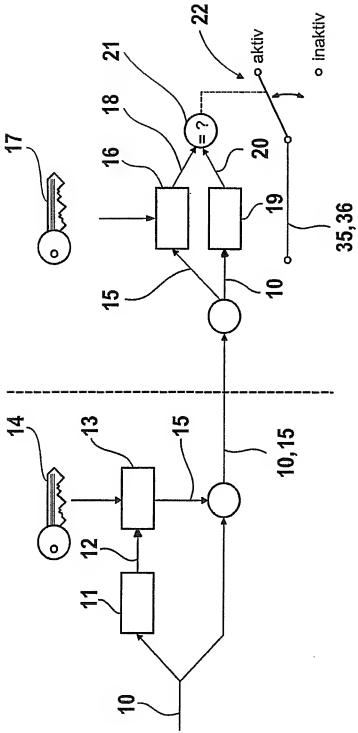


FIG. 2

Nummer: DE 101 26 451 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 5. Dezember 2002

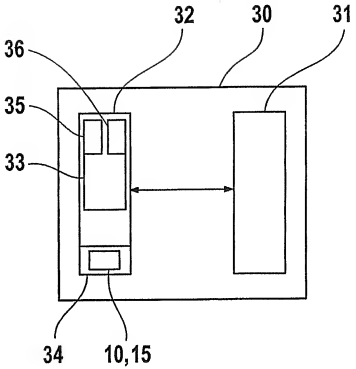


FIG. 3